PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-239779
(43)Date of publication of application : 12.09.1995

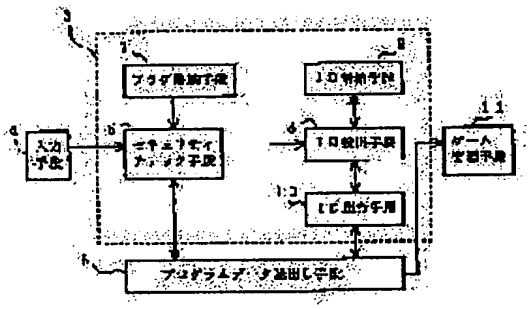
(51)Int.CI. G06F 9/06
G06F 12/14
G06F 12/14

(21)Application number : 06-030590
(22)Date of filing : 28.02.1994

(71)Applicant : SEGA ENTERP LTD
(72)Inventor : OOBA AKIHIRO
ASAI TOSHINORI

(54) DATA SECURITY DEVICE

(57)Abstract:
PURPOSE: To provide a data security device which facilitates the execution of data by person who has right authority while surely preventing the execution, analysis, copying, etc., of data on a recording medium by unauthorized person.
CONSTITUTION: An input means 4 is connected to a program read means 6 through a security check means 5. The program data read means 6 is connected to a game actualization means 11. A flag storage means 7 and an ID detecting means 8 are connected to the security check means 5. A security flag 7a and a read permission flag 7b are stored in the flag storage means 7. An ID storage means 9 and an ID matching means 10 are connected to the ID detecting means 8. The ID matching means 10 is connected to the program data read means 6.



LEGAL STATUS

[Date of request for examination]	28.02.2001
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3653709
[Date of registration]	11.03.2005
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報(A)　(11)特許出願公開番号

特開平7－239779

(43)公開日　平成７年(1995)９月12日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　9/06	５５０　Ｚ	7230－5B		
12/14	３１０　Ｂ			
	３２０　Ａ			

審査請求　未請求　請求項の数６　ＯＬ　（全９頁）

(21)出願番号　特願平6－30590

(22)出願日　平成６年(1994)２月28日

(71)出願人　000132471
株式会社セガ・エンタープライゼス
東京都大田区羽田１丁目２番12号

(72)発明者　大場　聡宏
東京都大田区羽田１丁目２番12号　株式会社セガ・エンタープライゼス内

(72)発明者　浅井　敏典
東京都大田区羽田１丁目２番12号　株式会社セガ・エンタープライゼス内

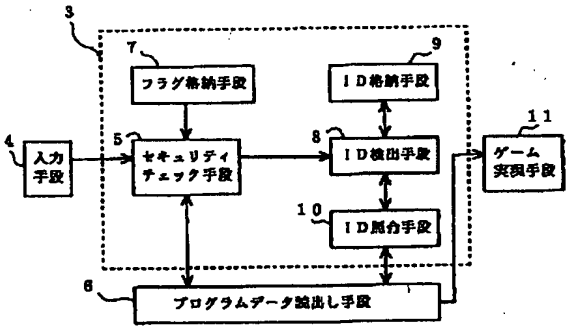
(74)代理人　弁理士　木内　光春

(54)【発明の名称】　データセキュリティ装置

(57)【要約】

【目的】　正当な権原の無い者による記録媒体内のデータの実行、解析、コピー等を確実に防止しつつ、正当な権原のある者によるデータの実行を容易にするデータセキュリティ装置を提案する。

【構成】　入力手段４を、セキュリティチェック手段５を介してプログラムデータ読み出し手段６に接続する。プログラムデータ読出し手段６をゲーム実現手段１１に接続する。セキュリティチェック手段５にフラグ格納手段７、ＩＤ検出手段８を接続する。フラグ格納手段７にセキュリティフラグ７ａ、読み出し許可フラグ７ｂを格納する。ＩＤ検出手段８にＩＤ格納手段９、ＩＤ照合手段１０を接続する。ＩＤ照合手段１０をプログラムデータ読出し手段６に接続する。



1

【特許請求の範囲】

【請求項1】　メインデータを処理するためのデータ処理装置に設けられ、メインデータ用の記憶媒体からメインデータを入力する入力手段と、前記入力手段により入力された前記メインデータを実行するデータ実行手段と、所定の処理を施された前記メインデータの読み出しのみを許可するセキュリティチェック手段とを備えたデータセキュリティ装置において、

前記セキュリティチェック手段における前記読出し手段の制御機能を解除する解除データ用の記憶媒体から、前記入力手段により入力された解除データに基づいて、前記セキュリティチェック手段の制御機能を解除する解除手段を設けたことを特徴とするデータセキュリティ装置。

【請求項2】　前記メインデータ用の記憶媒体および前記解除データ用の記憶媒体は、前記データ処理装置に着脱自在に設けられていることを特徴とする請求項1記載のデータセキュリティ装置。

【請求項3】　前記メインデータ用の記憶媒体および前記解除データ用の記憶媒体には、同一または異なるＩＤデータが格納され、

前記入力手段により入力されたＩＤデータを検出するＩＤ検出手段と、

前記ＩＤ検出手段により検出されたＩＤデータを格納するＩＤ格納手段と、

前記メインデータ用の記憶媒体に格納されたＩＤデータと前記解除データ用の記憶媒体に格納されたＩＤデータとが同一の場合にのみ前記読出し手段を作動させるＩＤ照合手段とを有することを特徴とする請求項2記載のデータセキュリティ装置。

【請求項4】　前記解除手段は、前記セキュリティチェック手段の機能の作動を制御するフラグと、

前記フラグを格納したフラグ格納手段とを有することを特徴とする請求項3記載のデータセキュリティ装置。

【請求項5】　前記メインデータはゲームのプログラムデータであり、

前記データ処理装置はコンピュータを有するゲーム機であり、

前記解除手段、前記フラグ格納手段、前記ＩＤ検出手段、前記ＩＤ格納手段および前記ＩＤ照合手段を前記ゲーム機のコンピュータ上に構成したことを特徴とする請求項4記載のデータセキュリティ装置。

【請求項6】　前記メインデータ用の記憶媒体および前記解除データ用の記憶媒体はＣＤ－ＲＯＭであり、

前記入力手段はＣＤ－ＲＯＭドライブであることを特徴とする請求項5記載のデータセキュリティ装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、たとえばゲームのプログラムデータを記録したＲＯＭの内容が、違法に実行、

2

コピーまたは解析されることを防止するデータセキュリティ装置に関する。

【０００２】

【従来の技術】初期の頃の単純なテレビゲーム機は、本体内に固定されたメモリにゲームのプログラムデータが記録され、このプログラムによって実現されるゲームだけを楽しむことしかできなかった。しかし、近年では、ゲームのプログラムデータを記録したＲＯＭを、ゲーム機本体に着脱自在に設け、このＲＯＭを交換するだけで様々な異なったゲームを楽しむことができるゲーム機が開発され、広く普及している。このようなＲＯＭは、ＲＯＭカートリッジのように専用の回路を小ケース内に封入したカートリッジ型のもの、ＣＤ－ＲＯＭのように光学記録媒体を使用したものなどがあり、それぞれの利点を生かした利用がなされている。

【０００３】そして、特に人気のあるゲームプログラムを記録したＲＯＭカートリッジやＣＤ－ＲＯＭは、商品の供給が需要に対応できず、高額で取り引きされることが多い。このため、ＲＯＭの内容が違法にコピーされ、市場に出回るケースが後を絶たない。また、ゲームセンターにおけるアーケードゲーム機の場合には、ゲームプログラムを記録したＲＯＭとして、基板上の回路によって構成したＲＯＭボードが用いられている。このようなＲＯＭボードも、本体に着脱自在に設けられているので、内容が違法にコピーされ、業務用として盗用される可能性が高い。

【０００４】これに対処するため、通常のＲＯＭのデータには、解析やコピーを制限する処理が施され、ゲーム機側には、この処理のなされていないＲＯＭ内のゲームプログラムの実行を制限するデータセキュリティ装置が設けられている。このようなデータセキュリティ装置の一例として、ＣＤ－ＲＯＭ用のゲーム機に設けたものを以下に説明する。

【０００５】まず、通常に市販されているＣＤ－ＲＯＭ（以下、市販ＣＤと呼ぶ）に記録されたデータは、以下のように構成されている。すなわち、図7に示すように、市販ＣＤ内には、ゲームのプログラムデータ１８ｄが記録され、さらに、専用の装置でなければ解析、コピーが不可能な特殊コード１８ａが挿入されている。

【０００６】一方、市販のゲーム機のコンピュータ上には、市販ＣＤ内の特殊コード１８ａの有無をチェックして、特殊コード１８ａのあるプログラムのみの実行を許可するセキュリティチェック手段が設けられている。すると、特殊コード１８ａが挿入されている正規の市販ＣＤならば、セキュリティチェック手段によってプログラムデータ１８ｄの実行が許可されるので、通常の市販のゲーム機でゲームのプログラムデータ１８ｄを実行することができる。そして、市販ＣＤ内のプログラムデータ１８ｄが違法にコピーされた場合であっても、特殊コード１８ａはコピーされないので、そのＣＤ内のプログラ

ムデータ１８ｄを市販のゲーム機で実行しようとしても、セキュリティチェック手段が存在するために実行できないことになる。

【０００７】

【発明が解決しようとする課題】しかしながら、上記のような従来のデータセキュリティ装置には、以下のような問題点があった。すなわち、ゲームのプログラムデータの内容は、正当な権原を有しない者による違法なコピー、解析または実行からは、確実に保護されるべきであるが、ゲームプログラムの正規の開発者（正当な権原を有する者）は、内容を容易に実行できる方が便利である。なぜなら、作成したゲームがどの様に実行されるかを常にチェックする必要があるからである。そして、このチェックに用いる装置は、専用の装置を作ることによって余計な費用をかけるよりも、ユーザーが使用するものと同一の市販の装置でおこなう方がよい。ユーザーの立場からゲームを楽しむことができるかどうかをチェックする意味からも、市販のゲーム機でおこなうことが望ましいのである。

【０００８】しかし、上述のように、市販のゲーム機は特殊コードの有無をチェックするセキュリティチェック手段が存在するので、特殊コードがない開発中のゲームプログラムを実行することができない。さらに、特殊コードは、解析やコピー不能とするために、非常に複雑な構成を有しているので、作成する場合には、かなりの時間と手間がかかり、ゲームソフトを開発する度に作成しているとゲームプログラムの開発に支障をきたす可能性がある。

【０００９】本発明は、以上のような従来技術の課題を解決するために提案されたものであり、その目的は、正当な権原の無い者によるデータの実行、解析、コピー等を確実に防止しつつ、権原のある者によるデータの実行を容易におこなうことができるデータセキュリティ装置を提案することである。

【００１０】

【課題を解決するための手段】上記の目的を達成するために、請求項１記載の発明は、メインデータを処理するためのデータ処理装置に設けられ、メインデータ用の記憶媒体からメインデータを入力する入力手段と、前記入力手段により入力された前記メインデータを実行するデータ実行手段と、所定の処理を施された前記メインデータの読み出しのみを許可するセキュリティチェック手段とを備えたデータセキュリティ装置において、前記セキュリティチェック手段における前記読出し手段の制御機能を解除する解除データ用の記憶媒体から、前記入力手段により入力された解除データに基づいて、前記セキュリティチェック手段の制御機能を解除する解除手段を設けたことを特徴とする。

【００１１】請求項２記載の発明は、請求項１記載のデータセキュリティ装置において、前記メインデータ用の

記憶媒体および前記解除データ用の記憶媒体は、前記データ処理装置に着脱自在に設けられていることを特徴とする。

【００１２】請求項３記載の発明は、請求項２記載のデータセキュリティ装置において、前記メインデータ用の記憶媒体および前記解除データ用の記憶媒体には、同一または異なるＩＤデータが格納され、前記入力手段により入力されたＩＤデータを検出するＩＤ検出手段と、前記ＩＤ検出手段により検出されたＩＤデータを格納するＩＤ格納手段と、前記メインデータ用の記憶媒体に格納されたＩＤデータと前記解除データ用の記憶媒体に格納されたＩＤデータとが同一の場合にのみ前記読出し手段を作動させるＩＤ照合手段とを有することを特徴とする。

【００１３】請求項４記載の発明は、請求項３記載のデータセキュリティ装置において、前記解除手段は、前記セキュリティチェック手段の機能の作動を制御するフラグと、前記フラグを格納したフラグ格納手段とを有することを特徴とする。

【００１４】請求項５記載の発明は、請求項４記載のデータセキュリティ装置において、前記メインデータはゲームのプログラムデータであり、前記データ処理装置はコンピュータを有するゲーム機であり、前記解除手段、前記フラグ格納手段、前記ＩＤ検出手段、前記ＩＤ格納手段および前記ＩＤ照合手段を前記ゲーム機のコンピュータ上に構成したことを特徴とする。

【００１５】請求項６記載の発明は、請求項５記載のデータセキュリティ装置において、前記メインデータ用の記憶媒体および前記解除データ用の記憶媒体はＣＤ－ＲＯＭであり、前記入力手段はＣＤ－ＲＯＭドライブであることを特徴とする。

【００１６】

【作用】上記のような構成を有する本発明の作用は以下の通りである。すなわち、請求項１記載の発明では、メインデータ用の記憶媒体からメインデータを入力手段により入力すると、解除手段によってセキュリティチェック手段における読出し手段の制御機能が解除される。すると、メインデータ用の記憶媒体から入力手段によってメインデータが入力された場合に、読出し手段がメインデータを読み出し、メインデータが実行手段に送られる。したがって、所定の処理が施されていないメインデータであっても、あらかじめ解除データを入力しておくことによって、実行可能となる。

【００１７】請求項２記載の発明では、メインデータ用の記憶媒体がデータ処理装置に着脱自在に設けられているので、ユーザーによる広範な利用が実現できる。そして、かかる記憶媒体のメインデータが、正当な権原の無いものに不当にコピーされた等の事情により所定の処理を施されていないものとなった場合には、セキュリティチェック手段における読出し手段の制御機能が働くの

5

で、データ処理装置によってデータを不当に実行することはできない。

【0018】一方、解除データ用の記憶媒体がデータ処理装置に着脱自在に設けられているので、解除データ用の記憶媒体を正当な権原を有する者が秘匿しておけば、正当な権原を有する者のみが試作中のデータを実行することができる。すなわち、解除データ用の記憶媒体をデータ処理装置に装着すれば、上記のようにセキュリティチェック手段における読出し手段の制御機能を解除することができる。したがって、このような解除後に、試作中である等の事情で所定の処理を施されていないメインデータ用の記憶媒体をデータ処理装置に装着すれば、メインデータの実行をおこなうことができる。

【0019】請求項3記載の発明では、解除データ用の記憶媒体から入力手段により入力されたＩＤデータが、ＩＤ検出手段により検出され、ＩＤ格納手段に格納される。つぎに、メインデータ用の記憶媒体から入力手段により入力されたＩＤデータがＩＤ検出手段により検出され、ＩＤ格納手段に格納された解除データ用の記憶媒体のＩＤデータとメインデータ用の記憶媒体のＩＤデータとがＩＤ照合手段によって照合される。もし、ＩＤデータが一致すれば、読出し手段が作動し、メインデータ用の記憶媒体から入力手段によって入力されるとメインデータを読出し手段が読み出し、メインデータが実行手段に送られるので、メインデータが実行手段によって実行可能となる。

【0020】また、ＩＤデータが一致しなければ、読出し手段は作動せず、メインデータ用の記憶媒体からメインデータが入力手段によって入力されても、メインデータを読出し手段が読み出すことはないので、メインデータは実行されない。

【0021】請求項4記載の発明では、解除データ用の記憶媒体から入力手段により入力された解除データによって、フラグ格納手段に格納されたフラグのＯＮ、ＯＦＦをおこなう。そして、このフラグがＯＮとなることによってセキュリティチェック手段の作動を制御することができるので、プログラム上の手順によって解除手段を実現できる。

【0022】請求項5記載の発明では、はじめに、解除データ用の記憶媒体から入力手段によって解除データおよびＩＤデータを入力する。すると、上記のように、解除データによってセキュリティチェック手段の機能が解除され、ＩＤデータがＩＤ格納手段に格納される。つぎに、メインデータ用の記憶媒体から入力手段によってゲームのプログラムデータおよびＩＤデータを入力する。すると、上記のように、ＩＤ格納手段に格納されたＩＤデータとメインデータ用の記憶媒体のＩＤデータとが一致すれば、読出し手段が作動し、ゲームのプログラムデータが読み出され、実行手段によってゲームが実行される。

6

【0023】また、ＩＤデータが一致しなければ、読出し手段は作動せず、ゲームのプログラムデータを読出し手段が読み出すことはないのでゲームは実行されない。

【0024】請求項6記載の発明では、まず、解除データ用のＣＤ－ＲＯＭをＣＤ－ＲＯＭドライブに装着することにより、上記のようにセキュリティチェック手段の機能解除、ＩＤデータの格納がおこなわれる。つぎに、メインデータ用のＣＤ－ＲＯＭをＣＤ－ＲＯＭドライブに装着する（ＣＤ－ＲＯＭを交換する）ことにより、上記のようにゲームのプログラムデータの読み出し、実行がおこなわれる。

【0025】

【実施例】請求項1～請求項6記載の本発明に対応する一実施例を、図面にしたがって以下に説明する。なお、請求項1記載の読出し手段はプログラムデータ読出し手段、解除データはＫＥＹ－ＣＤデータ、メインデータ用の記憶媒体は試作ＣＤまたは市販ＣＤ、解除データ用の記憶媒体はＫＥＹ－ＣＤとする。請求項3記載のＩＤデータはＫＥＹ－ＩＤおよびＤＩＳＣ－ＩＤとし、請求項4記載のフラグはセキュリティフラグとする。また、請求項1におけるメインデータに施す所定の処理とは、同一のＣＤ内に特殊コードを挿入することを意味する。

【0026】さらに、本実施例は、テレビゲーム機のコンピュータ上に実現されるものであり、装置の各機能は、プログラムの形式で表現された所定の手順でコンピュータを動作させることによって実現されているが、本装置の機能の全部又は一部は専用の電子回路上に実現してもよい。以下、本装置の各機能を手段等によって表現したブロック図、およびハードウェア構成を示す仮想的回路ブロック図を用いて説明する。なお、本実施例におけるゲーム実現手段であるゲーム機の回路は、周知の技術によって構成されているので、説明を省略する。

【0027】（1）実施例の構成

本実施例の構成を以下に説明する。まず、試作中のＣＤ－ＲＯＭ（以下、試作ＣＤ１と呼ぶ）内のデータ構成を説明する。すなわち、図１に示すように、試作ＣＤ１には、ゲームのプログラムデータ１ｄとともに、制作するメーカーごとに異なった識別子であるＤＩＳＣ－ＩＤ１ｂが記録されている。そして、この試作ＣＤには、制作の手間を省き、作業効率を良くするために、特殊コードは挿入されていない。本実施例では、このような特殊コードの無い試作ＣＤ１であっても、プログラムの実行をおこなうことができるようにするために、試作ＣＤ１とは別個のＣＤ－ＲＯＭであるＫＥＹ－ＣＤ２を用いる。つまり、ゲーム機のＣＤドライブに、まずＫＥＹ－ＣＤ２をセットし、ＫＥＹ－ＣＤ２内のデータの読み出しをおこなうことによりセキュリティチェック手段の機能を解除する。その後に、ＣＤドライブ内のＫＥＹ－ＣＤ２を試作ＣＤ１に入れ替えて、試作ＣＤ１内のデータの読み出しをおこなう。

7

【0028】このようなセキュリティチェック手段の機能解除に用いられるKEY－CD2内の、データ構成を以下に説明する。すなわち、図2に示すように、KEY－CD2内には、専用の装置でなければ解析、コピーが不可能な特殊コード2aが挿入されている。この特殊コード2aは、従来例と同様に、入力されると市販のゲーム機に設けられたセキュリティチェック手段が、ゲームプログラムの読み出しを許可するデータである。また、KEY－CD2内には、ゲームプログラムを制作するメーカーごとに異なった識別子であるKEY－ID2bが記録されている。同じメーカーのKEY－ID2bとDISC－ID1bとは対応している。そして、KEY－CD2内には、セキュリティチェック手段が特殊コードの有無をチェックする機能を解除するKEY－CDデータ2cが記録されている。さらに、KEY－CD2には、プログラムデータ2dが記録されている場合もある。

【0029】一方、ゲーム機内に設けられたセキュリティ部3は、以下のような構成となっている。すなわち、図3に示すように、CD－ROM内の情報を入力するための入力手段4が、セキュリティチェック手段5を介してプログラムデータ読み出し手段6に接続されている。このセキュリティチェック手段5は、CD内の特殊コードの有無をチェックして、プログラムデータ読み出し手段6のプログラムデータの読み出しを制御する機能を有する。プログラムデータ読出し手段6は、ゲーム実現手段11に接続されている。このプログラムデータ読出し手段6は、CD内のプログラムデータを読み出して、ゲーム実現手段11に出力する機能を有する。

【0030】また、セキュリティチェック手段5には、CD内のDISC－ID1bおよびKEY－ID2bを検出するための手段であるID検出手段8が接続されている。ID検出手段8には検出されたKEY－ID2bを格納するためのID格納手段9が接続されている。また、ID検出手段8には、検出されたDISC－ID1bおよびID格納手段9に格納されたKEY－ID2bを照合するID照合手段10が接続され、ID照合手段10はプログラムデータ読出し手段6に接続されている。

【0031】さらに、セキュリティチェック手段5にはフラグ格納手段7が接続されている。このフラグ格納手段7には、図4に示すように、セキュリティフラグ7aおよび読み出し許可フラグ7bが格納されている。ここで、フラグとは、プログラム上のスイッチ点を制御する標識である。セキュリティフラグ7aはONとなる（フラグを立てる）ことによって、セキュリティチェック手段5の特殊コードチェック機能を作動可能な状態にするフラグである。また、読み出し許可グラフ7bは、ONとなることによって、プログラムデータ読み出し手段6のプログラムデータ読み出し機能を作動可能な状態とするフラグである。なお、後述の作用に示す処理手順をおこなうことができるように、所定のプログラムによって、以下のように設定されている。すなわち、ゲーム機本体の電源をONにした直後には、セキュリティフラグ7aはONとなり、読み出し許可グラフ7bはOFFとなるように設定され、KEY－ID2bがID格納手段に格納された後には、KEY－CDデータ2cによって、セキュリティフラグ7aはOFFとなり、読み出し許可グラフ7bはONとなるように設定されている。さらに、KEY－ID2bとDISC－ID1bが照合されて一致した後にも、読み出し許可フラグ7bがONとなるように設定されている。

8

【0032】なお、本実施例のハードウェア構成の簡略図を、以下に説明する。すなわち、図5に示すように、入力手段4としては、CD－ROMドライブ（以下、CDドライブ12と呼ぶ）が用いられる。このCDドライブ12には、プログラムデータ読み出し手段6を実現するCDドライブ制御回路13が接続されている。CDドライブ制御回路13は、CDデータバッファ14を介してゲームの実現手段11としてのゲーム機の回路15に接続されている。CDドライブ制御回路13には、セキュリティチェック手段5、ID検出手段8、ID照合手段10を実現するセキュリティ回路16が接続されている。セキュリティ回路16には、フラグ格納手段7およびID格納手段9を実現するメモリ17が接続されている。

【0033】（2）実施例の作用

以上のような構成を有する本実施例の作用を、図6の処理の手順を示すフローチャートにしたがって以下に説明する。すなわち、まずはじめに電源をONにする（ステップ501）。すると、セキュリティフラグ7aはONとなり（ステップ502）、読み出し許可フラグ7bはOFFとなる（ステップ503）。つぎに、ユーザーがCDドライブ12にKEY－CD2をセットすると、セキュリティチェック手段5によって、セキュリティフラグ7aがチェックされる。この場合、セキュリティフラグ7aがONなので、ステップ505へ進む（ステップ504）。そして、セキュリティチェック手段5によって、KEY－CD2内の特殊コード2aの有無がチェックされる。セットされたKEY－CD2には、特殊コード2aが有るので、ステップ506に進む（ステップ505）。ID検出手段8によって、セットされたCDがKEY－CD2かどうかが判断される（ステップ506）。そして、KEY－CD2からKEY－ID2bが検出され、検出されたKEY－ID2bはID格納手段9に格納される（ステップ507）。KEY－ID2bがID格納手段9に格納されると、KEY－CDデータ2cによって、セキュリティフラグ7aがOFFになり（ステップ508）、読み出し許可フラグ7bがONになる（ステップ509）。

9

【００３４】つぎに、ユーザーがＣＤドライブ１２内のＫＥＹ－ＣＤ２を試作ＣＤ１に交換すると、ＣＤの交換がおこなわれたことが検出され（ステップ５１０）、ステップ５０３に戻ってそれ以降の処理をおこなう。そして、この場合、すでにステップ５０８においてセキュリティフラグ７がＯＦＦとなっているので、ステップ５０４からステップ５１４に進み、ＩＤ検出手段８によって試作ＣＤ１内のＤＩＳＣ－ＩＤ１ｂが検出される。検出されたＤＩＳＣ－ＩＤ１ｂとＩＤ格納手段９に格納されたＫＥＹ－ＩＤ２ｂとは、ＩＤ照合手段１０によって照合される（ステップ５１４）。ＤＩＳＣ－ＩＤ１ｂとＫＥＹ－ＩＤ２ｂとが、同一メーカーのＩＤであって一致する場合には、ステップ５１６に進み（ステップ５１５）、読み出し許可フラグ７ｂがＯＮになる（ステップ５１６）。

【００３５】この後は、試作ＣＤ１はそのままＣＤドライブ１２にセットしておくので、ＣＤの交換はおこなわれなかったことになり、ステップ５１１へ進む（ステップ５１０）。プログラムデータ読み出し手段６は、所定のプログラムにより設定された読み出し用のコマンドを受信した場合には、ステップ５１２に進み、コマンドの受信がない場合には、ステップ５１０に戻る（ステップ５１１）。コマンド受信後は、読み出し許可フラグ７ｂがＯＮかどうかがチェックされる。つまり、試作ＣＤ１のＤＩＳＣ－ＩＤ１ｂがＫＥＹ－ＣＤ２のＫＥＹ－ＩＤ２ｂと一致する場合には、ステップ５１６において読み出し許可フラグ７ｂがＯＮとなっているので、ステップに５１３に進む。以上のような手順を経て、プログラムデータ読み出し手段６によって、試作ＣＤ１内のプログラムデータ１ｄを読み出すことが可能となり（ステップ５１３）、ゲームプログラムがゲーム機の回路１５に出力されることによりゲームが実行される。

【００３６】また、ステップ５１５において、試作ＣＤ１のＤＩＳＣ－ＩＤ１ｂがＫＥＹ－ＣＤ２のＫＥＹ－ＩＤ１ｂと一致しない場合には、ステップ５０５へ戻る。つぎに、試作ＣＤ１には特殊コードがなく、ステップ５１０へと進むので、読み出し許可フラグ７ｂはＯＦＦのままである。そして、ステップ５１２において、読み出し許可フラグＯＦＦが判断されてステップ５１０に戻るので、ＫＥＹ－ＩＤ２ｂに一致するＤＩＳＣ－ＩＤ１ｂをもつ試作ＣＤ１がセットされるまで、プログラムデータ１ｄの読み出しはおこなわれない。

【００３７】なお、本実施例は、当然に従来例と同様に市販ＣＤ１８をセットしてゲームを実行することもできる。市販ＣＤ１８をセットしてゲームを実行する場合の手順は、以下の通りである。すなわち、市販ＣＤ１８には特殊コード１８ａが存在するので、ステップ５０１～ステップ５０５までは、上記例と同様に進む。つぎに、ステップ５０６においては、ＣＤドライブ１２にセットされた市販ＣＤ１８にはＫＥＹ－ＩＤはないので、ステップ５０９に進み、読み出し許可フラグ７ｂがＯＮになる。これ以降の手順は上記試作ＣＤ１の場合と同様であり、前記のようにステップ５０９において読み出し許可フラグ７ｂがＯＮになっているので、プログラムデータ１８ｄの読み出しがおこなわれる（ステップ５１０～５１３）。

10

【００３８】さらに、違法にコピーされたＣＤ－ＲＯＭの場合（以下、違法コピーＣＤと呼ぶ）には、以下のような手順にしたがって、プログラムデータの読み出しが制限される。まず、違法コピーＣＤは、特殊コードが挿入されていない。このような違法コピーＣＤをＣＤドライブ１２にセットしても、ステップ５０１からステップ５０４までの手順が上記例と同様におこなわれる。しかし、ステップ５０５において特殊コードの有無が判断されると、特殊コードがないのでステップ５１０に進む。その後の手順は試作ＣＤの場合と同様に進むが、読み出し許可フラグ７ｂはＯＦＦとなったままなので、ステップ５１２においてチェックされ、プログラムデータの読み出しはおこなわれない。

【００３９】（３）実施例の効果

以上のような本実施例の効果は、以下の通りである。すなわち、市販のゲーム機に本実施例を設けると、ＫＥＹ－ＣＤ２を用いることによって、セキュリティチェック手段５による特殊コードチェック機能をＯＦＦにすることができるので、試作ＣＤ１であって特殊コードのないものであっても、ゲームを実行することができる。したがって、ゲームソフトの開発中に、試作したゲームを市販のゲーム機によって容易に実行して試験、確認等をおこなうことができるので、開発を効率よく円滑におこなうことができる。

【００４０】また、違法コピーＣＤには特殊コードがないので、ＫＥＹ－ＣＤ２がない限り、市販のゲーム機でゲームを実行することはできず、ゲームプログラムの秘密保持は守られる。

【００４１】また、解除手段は、機械的なスイッチによって実現することも可能であるが、フラグのＯＮ、ＯＦＦというプログラム上の手法によって実現できるので、設定の変更等が容易におこなえる。

【００４２】また、ＫＥＹ－ＣＤ２内に記録されたＫＥＹ－ＩＤ２ｂは、試作ＣＤ１内のＤＩＳＣ－ＩＤ１ｂと一致しなければゲームを実行することができない。したがって、各開発メーカーごとにまたは各開発者ごとに異なったＫＥＹ－ＣＤ２を持つようにすれば、ＫＥＹ－ＣＤ２を、どんなＣＤでも読み出し可能にするマスターキーとして使用することはできないので、秘密保持の確実性は高い。

【００４３】さらに、セキュリティチェック手段５の機能解除用のＫＥＹ－ＣＤデータ２ｃおよびＩＤ照合用のＫＥＹ－ＩＤ２ｂは、一枚のＫＥＹ－ＣＤ２に記録されているので、ＫＥＹ－ＣＤデータ２ｃやＫＥＹ－ＩＤ２

bの入力に手間がかからず便利である。また、ゲームのプログラムデータ1dおよびDISC－ID1bは、一枚の試作CD1に記録されているので、DISC－ID1bの入力とプログラムデータ1dの入力とを別々におこなう必要がない。よって、開発者は試作CD1のチェックを容易に迅速におこなうことができ、ゲーム開発の効率が向上する。

【0044】（4）その他の実施例

本発明は、以上のような実施例に限定されるものではなく、各機能ブロックの接続、配置および設定等は適宜変更可能である。たとえば、KEY－CD2内のプログラムデータ2dは、必ずしも必要ではない。また、試作CD1内のDISC－ID1bおよびKEY－CD2内のKEY－ID2bを複数設定し、すべてのIDが一致しなければプログラムデータを読み出すことができないように設定すれば、秘密保持の確実性はさらに増す。

【0045】なお、特殊コードによるセキュリティのみでよい場合には、上述のDISC－ID1bおよびKEY－ID2bを用いない設定にすることもできる。この場合、CD－ROM内にこれらのIDを格納する必要もなく、ゲーム機にもID検出手段8等を設ける必要がなくなり、KEY－CD2はいわゆるマスターキーのように使用することができる。

【0046】また、本発明は、ゲーム機ばかりでなく、通常のコンピュータにおけるデータセキュリティ装置として用いることもできる。したがって、記憶媒体としてCD－ROM以外のもの、たとえば、ROMカートリッジ、ROMボード、フロッピーディスク、RAMカード、磁気テープ、光磁気ディスク等であってもよい。また、入力手段4はCDドライブ12以外の装置、例えば、フロッピーディスクドライブ、RAMカード装置、磁気テープ装置、光学ディスク装置、磁気ディスク装置などを用いてもよい。

【0047】フラグ格納手段7やID格納手段9等の格納手段は、実現の態様は自由であり、たとえば、主記憶装置上に実現しても外部記憶装置上に実現してもよく、CPUのレジスタやキャッシュメモリを用いてもよい。また、フラグ格納手段7やID格納手段9等は実現されるメモリ17が、同種か別種かも自由である。

【0048】解除手段は、フラグのON、OFFによるばかりでなく、他のプログラム上の手法によっても実現できるし、上述のように機械的なスイッチによって実現することも可能である。

【0049】さらに、本実施例における各手順の各ステップは、その性質に反しない限り、実行順序を変更し、複数同時に実行し、また、実行ごとに異なった順序で実行してもよい。

【0050】

【発明の効果】以上のような本発明によれば、セキュリティチェック手段の機能を一時的に解除するスイッチ手段を設けることによって、正当な権原の無い者による記録媒体内のデータの実行、解析、コピー等を確実に防止しつつ、正当な権原のある者によるデータの実行を容易にするデータセキュリティ装置を提案することができる。

【図面の簡単な説明】

【図1】本発明の一実施例に使用する試作CDのデータ構成を示す説明図

【図2】本発明の一実施例に使用するKEY－CDのデータ構成を示す説明図

【図3】本発明の一実施例の構成を示すブロック図

【図4】図3の実施例におけるフラグ格納手段の内容を示す説明図

【図5】図3の実施例における回路ブロック図

【図6】図3の実施例の処理の手順を示すフローチャート

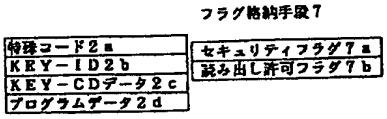
【図7】市販CDのデータ構成を示す説明図。

【符号の説明】

1…試作CD
1b…DISC－ID
1d…プログラムデータ
2…KEY－CD
2a…特殊コード
2b…KEY－ID
2c…KEY－CDデータ
2d…プログラムデータ
3…セキュリティ部
4…入力手段
5…セキュリティチェック手段
6…プログラムデータ読出し手段
7…フラグ格納手段
7a…セキュリティフラグ
7b…読み出し許可フラグ
8…ID検出手段
9…ID格納手段
10…ID照合手段
11…ゲーム実現手段
12…CDドライブ
13…CDドライブ制御回路
14…CDデータバッファ
15…ゲーム機の回路
16…セキュリティ回路
17…メモリ
18…市販CD
18a…特殊コード
18d…プログラムデータ
501以降…手順の各ステップ

【図1】

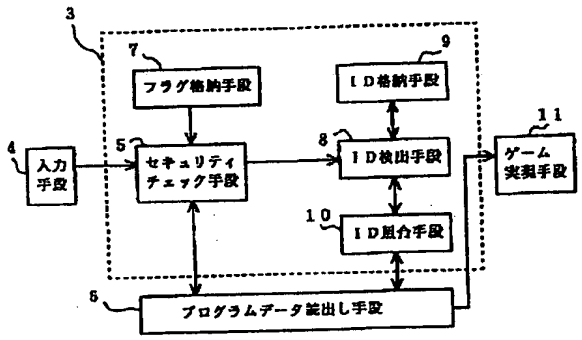
【図2】



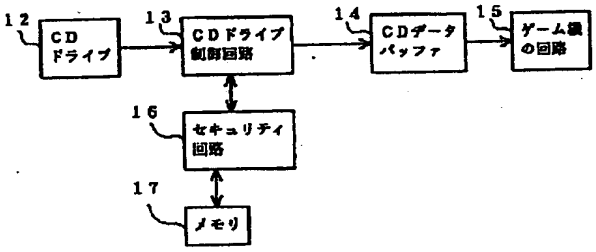
【図4】

【図7】

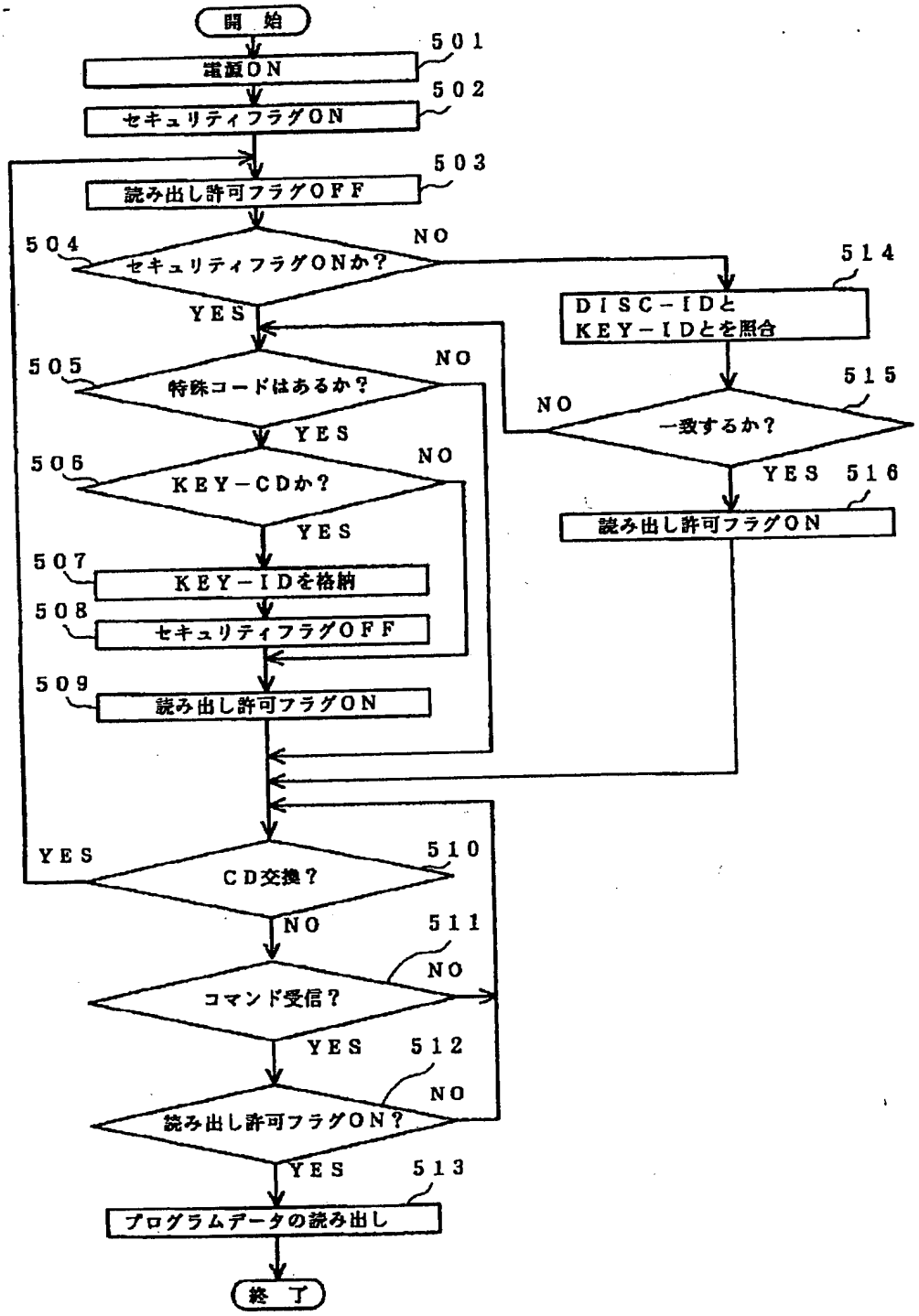
【図3】



【図5】



【図6】


開　始
501
電源ON
502
セキュリティフラグON
503
読み出し許可フラグOFF
504
セキュリティフラグONか？
NO
YES
514
DISC－IDと
KEY－IDとを照合
505
特殊コードはあるか？
NO
YES
515
一致するか？
NO
YES
506
KEY－CDか？
NO
YES
516
読み出し許可フラグON
507
KEY－IDを格納
508
セキュリティフラグOFF
509
読み出し許可フラグON
YES
510
CD交換？
NO
511
コマンド受信？
NO
YES
512
読み出し許可フラグON？
NO
YES
513
プログラムデータの読み出し
終　了